

JAN 29 2007

REMARKS**Introduction**

In the Office Action mailed October 30, 2006, the Examiner: (1) rejected claims 1-10 under 35 U.S.C. § 101 as being drawn to unpatentable subject matter; (2) rejected claims 1-10 under 35 U.S.C § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention; and (3) rejected claims 11-20 under 35 U.S.C. § 102(e) as being anticipated by Rothermel et al., U.S. Patent 6,678,827 ("Rothermel"). Applicants request reconsideration and allowance of the rejected claims in light of the amendments and the reasons described below.

1. Amendment to Claim 17 to Correct a Typographical Error

Applicants have amended claim 17 to correct a typographical error. In particular, Applicants amended claim 17 to replace the previously recited "using to database engine providing deduction to associate the one or more security goals with the at least one network device" with the currently amended "using to the database engine providing deduction to associate the one or more security goals with the at least one network device."

2. Response to the 35 U.S.C. § 101 Rejections

The Examiner rejected claims 1-10 under 35 U.S.C. § 101 because a "reference model for use in configuring security software on a computer" does not produce a tangible result. (Office Action, pp. 2-3) Applicants have amended claims 1-10 as set forth below and submit that the amended claims comply with 35 U.S.C. § 101.

(a) Claims 1-3

Applicants have amended claims 1-3 to replace the previously claimed "network reference model for use in configuring security software" with the currently amended "system for configuring security software." Applicants therefore submit that amended claims 1-3 comply with 35 U.S.C. § 101 because Applicants' claimed "system for configuring security software" is a "new and useful...machine" under 35 U.S.C. § 101.

(b) Claims 4-10

Applicants have amended claims 4-10 to clarify that the previously claimed "configuration tool for use in configuring security software packages" is a currently amended "configuration tool implemented on a computer-readable medium for use in configuring security software packages" as directed by the Examiner. (Office Action, p. 3) Applicants therefore submit that amended claims 4-10 comply with 35 U.S.C. § 101 because Applicants' currently amended "configuration tool implemented on a computer-readable medium for use in configuring security software packages" is a "new and useful...machine" under 35 U.S.C. § 101.

3. Response to the 35 U.S.C. § 112, Second Paragraph, Rejections

The Examiner rejected claims 1-10 under 35 U.S.C § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. (Office Action, p. 3) Applicants have amended claims 1-10 as set forth below and submit that the amended claims comply with 35 U.S.C. § 112, second paragraph.

(a) Claims 1, 4, and 10

Claims 1, 4, and 10 originally claimed, *inter alia*, "uses that the hardware and software of the network may support." The Examiner stated that the claim element "may" renders the scope of the limitation indefinite. (Office Action, p. 3) Applicants submit that "may" in the original claim is not indefinite as in "may or may not" but rather, "may" is permissive as in "permitted to." Applicants have amended claims 1, 4, and 10 to claim, *inter alia*, "uses that the hardware and software are permitted to support" to clarify the original claim language as directed by the Examiner. (Office Action, p. 3) Applicants therefore submit that amended claims 1, 4, and 10 comply with 35 U.S.C. § 112, second paragraph, because Applicants' currently amended claims particularly point out and distinctly claim the subject matter which Applicants regard as the invention.

(b) Claims 2, 6 and 10

Claims 2, 6, and 10 originally claimed, *inter alia*, "possible attacks against the network and benign events that could be confused with the possible attacks." The Examiner stated that the claim term "possible" renders the scope of the limitation indefinite. (Office Action, p. 4)

Applicants submit that the “possible attacks” as originally claimed is not indefinite as in attacks that may or may not occur, but rather, “possible attacks” are network events that the system identifies for further investigation, i.e., “suspected attacks.” Applicants have amended claims 2, 6, and 10 to claim, *inter alia*, “benign network events, suspected network attacks, and actual network attacks” to clarify the original claim language. Applicants therefore submit that amended claims 2, 6, and 10 now comply with 35 U.S.C. § 112, second paragraph, because Applicants’ currently amended claims particularly point out and distinctly claim the subject matter which Applicants regard as the invention.

(c) Claims 2-3, 5, and 7-9

The Examiner rejected claims 2-3, 5, and 7-9 as being dependent on base claims rejected under 35 U.S.C. § 112, second paragraph. (Office Action, p. 4) Applicants have amended independent claims 1 and 4 from which claims 2-3, 5, and 7-9 depend, thereby overcoming the Examiner’s 35 U.S.C. § 112, second paragraph, rejections as set forth above. Therefore, Applicants submit that claims 2-3, 5, and 7-9 no longer depend from rejected base claims.

4. Response to the 35 U.S.C. § 102(e) Rejections

The Examiner rejected claims 11-20 under 35 U.S.C. § 102(e) as being anticipated by Rothermel. (Office Action, p. 4) In response, Applicants submit that the rejection is improper and should be withdrawn because the Examiner’s cited reference does not disclose Applicants’ claimed: (1) “using active inference in a database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device”; (2) “using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device”; (3) “using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals”; (4) “using the database engine providing deduction to associate the one or more security goals with the at least one network device”; (5) “automatically classifying each of the hardware devices into one of the classes of hardware devices using a database engine providing deduction”; and (6) “decomposing the first security goals into second security goals for individual hardware devices using the database engine and the configuration of the hardware

devices and the software packages installed on the network.” The elements comprising these claims are described throughout the specification, including, e.g., and without reference to any particular element, paragraphs [0007-0011], [0016-0018], [0026-0030], and [0038].

(a) Claims 11-14

The Examiner stated that Security Policy Manager Device 110 in Fig. 1 and the description of Fig. 3B in col. 10, lines 44-65 of Rothermel disclose “using active inference in a database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device” as recited in Applicants’ claim 11. (Office Action, p. 5) However, as set forth below, the Examiner’s cited sections of Rothermel do not show or suggest that Security Policy Manager Device 110 is a “database engine” nor does Rothermel disclose Applicants’ claimed step of “using active inference in a database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device.”

First, Rothermel’s Security Policy Manager Device 110 is not a “database engine.” In contrast, Rothermel describes “using a security policy manager device to remotely manage multiple network security devices.” (Rothermel, col. 3, lines 24-25) Applicants find nothing in Rothermel that describes a database or a database engine of any kind.

Second, Rothermel does not disclose Applicants’ claimed step of “using active inference in a database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device” for at least the reason that Rothermel does not disclose a “database engine.” Moreover, the section of Rothermel cited by the Examiner describes combining “the security policy template 300 and the network profile 310 for network 1...to create the security policy 315 for network 1” by replacing “the ‘InformationServices’ alias in rule 301 with the network addresses listed for the ‘InformationServices’ alias in definition 311.” (Rothermel, col. 10, lines 44-65) Rothermel’s substitution of pre-defined values for variables in a template does teach Applicants’ claimed step of “using active inference in a database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device.”

Therefore, Applicants submit that Rothermel does not show or suggest each and every element recited in claim 11. Accordingly, Applicants submit that claim 11 is allowable over

Rothermel for at least the reasons set forth above. Claims 12-14 depend from claim 11. Therefore, Applicants further submit that claims 12-14 are allowable for at least the reason that they depend from an allowable claim.

(b) Claims 15-16

The Examiner stated that Security Policy Manager Device 110 in Fig. 1 and the description of Fig. 3B in col. 10, lines 44-65 of Rothermel disclose "using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device" as recited in Applicants' claim 15. (Office Action, p. 5) However, as set forth below, the Examiner's cited sections of Rothermel do not show or suggest that Security Policy Manager Device 110 is an "object-oriented description logic database engine" nor does Rothermel disclose Applicants' claimed step of "using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device."

First, Rothermel's Security Policy Manager Device 110 is not an "object-oriented description logic database engine." In contrast, Rothermel describes "using a security policy manager device to remotely manage multiple network security devices." (Rothermel, col. 3, lines 24-25) Applicants find nothing in Rothermel that describes a database or a database engine of any kind, much less an "object-oriented description logic database engine" as recited in Applicants' claim 15.

Second, Rothermel does not disclose Applicants' claimed step of "using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device" for at least the reason that Rothermel does not disclose an "object-oriented description logic database engine." Moreover, the section of Rothermel cited by the Examiner describes combining "the security policy template 300 and the network profile 310 for network 1...to create the security policy 315 for network 1" by replacing "the 'InformationServices' alias in rule 301 with the network addresses listed for the 'InformationServices' alias in definition 311." (Rothermel, col. 10, lines 44-65) Rothermel's substitution of pre-defined values for variables in a template does teach Applicants' claimed step of "using active inference in an object-oriented

description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device.”

Therefore, Applicants submit that Rothermel does not show or suggest each and every element recited in claim 15. Accordingly, Applicants submit that claim 15 is allowable over Rothermel for at least the reasons set forth above. Claims 16 depends from claim 15. Therefore, Applicants further submit that claim 16 is allowable for at least the reason that it depends from an allowable claim.

(c) Claim 17

The Examiner stated that Security Policy Manager Device 110 in Fig. 1 and the description of Fig. 3B in col. 10, lines 24-65 of Rothermel discloses Applicants’ claimed steps of: (1) “using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals”; and (2) “using the database engine providing deduction to associate the one or more security goals with the at least one network device.” (Office Action, p. 7) However, as set forth below, the Examiner’s cited sections of Rothermel do not show or suggest that Security Policy Manager Device 110 is a “database engine providing deduction” nor does the Examiner’s cited sections of Rothermel teach Applicants’ claimed steps of: (1) “using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals”; and (2) “using the database engine providing deduction to associate the one or more security goals with the at least one network device.”

First, Rothermel’s Security Policy Manager Device 110 is not a “database engine providing deduction.” In fact, nothing in Rothermel describes a database engine of any kind, much less a “database engine providing deduction.”

Second, the Examiner’s cited section of Rothermel does not disclose Applicants’ claimed step of “using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals” for at least the reason that Rothermel does not disclose a “database engine providing deduction.” Moreover, the section of Rothermel cited by the Examiner describes combining “the security policy template 300 and the network profile 310 for network 1...to create the security policy 315 for network 1” by replacing “the ‘InformationServices’ alias in rule 301 with the network addresses listed for the

'InformationServices' alias in definition 311." (Rothermel, col. 10, lines 44-65) Rothermel's substitution of pre-defined values for variables in a template does not teach Applicants' claimed step of "using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals."

Finally, the Examiner's cited section of Rothermel does not disclose Applicants' claimed step of "using the database engine providing deduction to associate the one or more security goals with the at least one network device" for at least the reason that Rothermel does not disclose a "database engine providing deduction." Moreover, the section of Rothermel cited by the Examiner describes combining "the security policy template 300 and the network profile 310 for network 1...to create the security policy 315 for network 1" by replacing "the 'InformationServices' alias in rule 301 with the network addresses listed for the 'InformationServices' alias in definition 311." (Rothermel, col. 10, lines 44-65) Rothermel's description of substituting pre-defined values for variables in a template does not teach Applicants' claimed step of "using the database engine providing deduction to associate the one or more security goals with the at least one network device."

Therefore, Applicants submit that Rothermel does not show or suggest each and every element recited in claim 17. Accordingly, Applicants submit that claim 17 is allowable over Rothermel for at least the reasons set forth above.

(d) Claims 18-20

The Examiner stated that Security Policy Manager Device 110 in Fig. 1, col. 6, lines 7-54, and col. 10, lines 8-24 of Rothermel discloses the steps of: (1) "automatically classifying each of the hardware devices into one of the classes of hardware devices using a database engine providing deduction"; and (2) "decomposing the first security goals into second security goals for individual hardware devices using the database engine and the configuration of the hardware devices and the software packages installed on the network." (Office Action, p. 8) However, as set forth below, the Examiner's cited sections of Rothermel do not show or suggest that Security Policy Manager Device 110 is a "database engine" or a "database engine providing deduction" nor does the Examiner's cited sections of Rothermel disclose Applicants' claimed steps of: (1) that Security Policy Manager Device 110 is used to perform the steps of: (1) "automatically classifying each of the hardware devices into one of the classes of hardware devices using a

database engine providing deduction”; and (2) “decomposing the first security goals into second security goals for individual hardware devices using the database engine and the configuration of the hardware devices and the software packages installed on the network.”

First, Rothermel’s Security Policy Manager Device 110 is neither a “database engine” nor a “database engine providing deduction” as recited in Applicants’ claim 18. In fact, Applicants find nothing in Rothermel that describes a database engine of any kind, much less a “database engine providing deduction.”

Second, the Examiner’s cited section of Rothermel does not disclose Applicants’ claimed step of “automatically classifying each of the hardware devices into one of the classes of hardware devices using a database engine providing deduction” for at least the reason that Rothermel does not disclose a “database engine providing deduction.”

Finally, the Examiner’s cited section of Rothermel does not disclose Applicants’ claimed “decomposing the first security goals into second security goals for individual hardware devices using the database engine and the configuration of the hardware devices and the software packages installed on the network” for at least the reason that Rothermel does not disclose a “database engine.” Furthermore, nothing in the Examiner’s cited section of Rothermel shows or suggests Applicants’ claimed step of “decomposing the first security goals into second security goals for individual hardware devices using the database engine and the configuration of the hardware devices and the software packages installed on the network.” To the contrary, Rothermel describes “generating... specific security policies for each of several NSDs” from “a single security policy template” by combining “the security policy template...with the network profile for that network.” (Rothermel, col. 10, lines 10-21) Rothermel’s description of combining security policy templates with network profiles is merely populating variables with pre-defined values which does not teach Applicants’ claimed step of “decomposing the first security goals into second security goals for individual hardware devices using the database engine and the configuration of the hardware devices and the software packages installed on the network.”

Therefore, Applicants submit that Rothermel does not show or suggest each and every element recited in claim 18. Accordingly, Applicants submit that claim 18 is allowable over Rothermel for at least the reasons set forth above. Claims 19-20 depend from claim 18.

JAN 29 2007

Therefore, Applicants further submit that claims 19-20 are allowable for at least the reason that they depend from an allowable claim.

Conclusion

Applicants submit that the present application is in condition for allowance, and notice to that effect is hereby requested. Should the Examiner feel that further dialog would advance the subject application to issuance, the Examiner is invited to telephone the undersigned at (312) 913-0001.

Respectfully submitted,

Dated: January 29, 2007

By: 

Jeffrey P. Armstrong
Reg. No. 54,967